IN THE CLAIMS:

Please re-write the claims to read as follows:

1. (Currently Amended)   Apparatus for tightly-coupling hardware data encryption
2   functions with software-based protocol decode processing within a pipelined processor of
3   a programmable processing engine in a network switch, the apparatus comprising:
4   an encryption execution unit contained within the pipelined processor;
5   an ALU contained within the pipelined processor;
6   an instruction decode stage (ID stage), [ALU,] in response to reading an opcode
7   [op-code], enables the encryption execution unit to read data from a memory shared by
8   the ALU and the encryption execution unit [pipelined processor], and for the encryption
9   execution unit to process the data read from the shared memory; and
10   a multiplexer to select as an output a result of processing by the encryption exe-
11   cution unit rather than a result of ALU processing.

1   2. (Original) The apparatus of Claim 1 wherein the encryption execution unit is an en-
2   cryption tightly coupled state machine (TCSM) unit that is selectively invoked within the
3   pipelined processor.

1 3. (Currently Amended) The apparatus of Claim 2, further comprising:

2   native encryption opcodes provided within an instruction set of the pipelined

3 processor to enable selective access to the encryption TCSM unit by software.

1 4. (Currently Amended) The apparatus of Claim 3, further comprising:

2   a plurality of busses internal to the pipelined processor and wherein a hardware

3 portion of the interface allows the encryption TCSM unit to utilize the internal buses in

4 response to decode processing of the native encryption opcodes.

1 5. (Currently Amended) The apparatus of Claim 4, further comprising: [wherein]

2   the pipelined processor is a microcontroller core (TMC) processor having a

3 multi-stage pipeline architecture that includes an instruction fetch stage, an instruction

4 decode stage, an execution stage and a memory write-back stage.

1   6. (Currently Amended) The apparatus of Claim 5, further comprising: [wherein]

2   the TMC processor further includes an arithmetic logic unit, at least one internal

3   register, an instruction fetch and decode unit and the encryption TCSM unit organized as

4   a data path.

1   7. (Currently Amended) The apparatus of Claim 5 wherein the encryption TCSM unit

2   comprises:

3   a data encryption standard (DES) functional component cooperatively coupled to

4   a sub-key generation functional component.

1   8. (Currently Amended) The apparatus of Claim 7 wherein the DES functional compo-

2   nent comprises:

3   state machine hardware used to execute each round of a DES function.

4

1   9. (Currently Amended) The apparatus of Claim 7, further comprising:

2   the sub-key generation functional component comprises state machine hardware

3   that generates a sub-key as needed for each round of a DES function.

1   10. (Currently Amended) A method for tightly-coupling hardware data encryption

2   functions with software-based protocol decode processing within a pipelined processor of

3   a programmable processing engine in a network switch, the method comprising the steps

4   of:

5   providing an encryption execution unit within the pipelined processor;

6   providing an ALU within the pipelined processor;

7   enabling, by an instruction decode stage (ID stage) [ALU] in response to read-

8   ing an opcode [op-code], the encryption execution unit to read data from a memory

9   shared by the ALU and the pipelined processor, and for the encryption execution unit to

10   process the data read from the memory; and

11   selecting as output the result of processing by the encryption execution unit rather

12   than selecting results from the ALU.

11. (Currently Amended) The method of Claim 10, further comprising:

having native encryption opcodes contained within an instruction set of the pipe-
lined processor; and

issuing the native encryption opcodes directly to the encryption execution unit to
substantially reduce encryption setup latency.

12. (Currently Amended) The method of Claim 11, further comprising:

[the steps of, wherein the pipelined processor is a microcontroller core (TMC) processor
having a multi-stage pipeline architecture that includes an instruction decode stage and an
execution stage:]
decoding the native encryption opcodes at the instruction decode stage; and
in response to the step of decoding, invoking the encryption execution unit to per-
form encryption/decryption functions at the execution stage.

13. (Currently Amended) The method of Claim 12, further comprising:

[the steps of, wherein the encryption/decryption functions are performed on plaintext
stored at the network switch:]
protocol processing of protocols contained in a [the] plaintext stored at the net-
work switch to determine an appropriate encryption algorithm;
upon determining the appropriate encryption algorithm, immediately starting an
operation to fetch initial keys needed to perform the encryption/decryption functions; and

8   upon fetching the keys, providing the keys to the encryption execution unit within

9   the TMC processor.

1   14. (Currently Amended) The method of Claim 13, further comprising:

2   including a plurality of high-performance busses internal to the TMC processor;

3   and

4   accessing the internal busses to simultaneously load an encryption key and store

5   a previous encryption result.

1   15. (Previously Presented) The method of Claim 12 further comprising the step of,

2   wherein the encryption execution unit is an encryption tightly coupled state machine

3   (TCSM) unit:

4   initializing the encryption TCSM unit in response to execution of a first instruc-

5   tion that defines the form of operation to be performed.

1   16. (Original) The method of Claim 15 wherein the encryption TCSM unit comprises a

2   data encryption standard (DES) functional component cooperatively coupled to a sub-key

3   generation functional component and wherein the step of initializing comprises the steps

4   of:

5   decoding a first portion of the first instruction to initialize the DES functional

6   component; and

7

7 decoding a second portion of the first instruction to initialize the sub-key genera-

8 tion functional component.

1 17. (Original) The method of Claim 16 further comprising the step of:

2 executing a second instruction having a micro-opcode field containing a native

3 encryption opcode that specifies loading an initial key from a memory into the sub-key

4 generation functional component of the encryption TCSM unit.

1 18. (Previously Presented) The method of Claim 17 further comprising the step of:

2 performing a DES function on a plaintext in response to execution of a third in-

3 struction having a micro-opcode field containing a native encryption code that specifies

4 loading of the plaintext into the DES functional component of the encryption TCSM unit

5 and initiating DES operations; and

6 upon completing the DES operations, storing a ciphertext result in an internal

7 register coupled to the DES functional component.

1 19. (Original) The method of Claim 18 further comprising the step of:

2 executing a fourth instruction to store the ciphertext results contained in the inter-

3 nal register to a location in the memory.

1   20. (Currently Amended) A programmable processing engine of a network switch com-

2   prising:

3   an input header buffer;

4   an output header buffer; and

5   a plurality of processing complex elements symmetrically arrayed into rows and

6   columns that are embedded between the input header buffer and an output header buffer,

7   each processing complex element comprising a microcontroller core having an encryp-

8   tion tightly coupled state machine (TCSM) unit that is selectively invoked in response to

9   an instruction decode stage (ID stage) [the microcontroller] reading an opcode [op-code];

10   and

11   a selector to select an output from either the microcontroller OR the TCSM.

---

1   21. (Currently Amended) A pipelined processor in a network switch, the processor

2   comprising:

3   an ALU internal to the processor responsive to a first set of opcodes;

4   an encryption execution unit internal to the processor having an encryption tightly

5   coupled state machine (TCSM) responsive to a second set of opcodes[,] ;

6   an instruction decode stage (ID stage) to decode an opcode, the ID stage [ALU],

7   in response to an [op-code] opcode of said second set of opcodes, transferring processing

8   to the encryption execution unit   [to process in response to said second set of opcodes];

9   a multiplexer to select output from the ALU OR from the encryption execution

10   unit.

1   22.   (Currently Amended) The processor of Claim 21, wherein the processor is a mi-

2   crocontroller core (TMC) processor and further comprises:

3   an instruction fetch stage;

4   [an instruction decode stage to decode an instruction fetched by the instruction

5   fetch stage;]

6   an execution stage to execute an [a decoded] instruction decoded by the ID stage;

7   and

8   a memory write-back stage to write a result of said execution stage to memory.

1   23.   (Currently Amended) The processor of Claim 21, further comprises:

2   one or more internal registers;

3   a bus operatively connecting the one or more internal registers to both the ALU

4   and the encryption execution unit; and

5   a multiplexer having inputs from both the ALU and the encryption execution unit,

6   the multiplexer outputting a selected input.

1   24.   (Previously Presented) The processor of Claim 21, wherein the encryption TCSM

2   unit comprises:

3   a data encryption standard (DES) functional component cooperatively coupled to

4   a sub-key generation functional component.

1 25. (Previously Presented) The processor of Claim 24, wherein the DES functional

2 component comprises:

3   a state machine that executes each round of a DES function.

1 26. (Previously Presented) The processor of Claim 24, wherein the sub-key genera-

2 tion functional component comprises:

3   a state machine that generates a sub-key as needed for each round of a DES

4 function.

1 27. (Currently Amended) A method for providing encryption functions within a pipe-

2 lined processor in a network switch, the method comprising the steps of:

3   associating a first set of opcodes with an ALU internal to the processor, the ALU

4 performing protocol processing operations;

5   associating a second set of opcodes with an encryption execution unit internal to

6 the processor, the encryption execution unit performing encryption operations;

7 [or having an encryption tightly coupled state machine (TCSM), wherein protocol proc-

8 essing operations are performed by the ALU and encryption operations are performed by

9 the encryption execution unit in response to said second set of opcodes; and]

11

10

11   decoding opcodes by an instruction decode stage (ID stage);

12   transferring by the ID stage, in response to an opcode from said first set of op-

13 codes, processing to the ALU;

14

15   transferring by the ID stage [ALU], in response to an [op-code] opcode from said

16 second set of opcodes, processing to the encryption execution unit

17 [to process encryption operations in response to said second set of opcodes]; and

18

19   selecting output from the ALU OR from the encryption execution unit.

1   28.   (Previously Presented) The method of Claim 27, further comprises the step of:

2   providing one or more internal registers;

3   providing a bus operatively connecting the one or more internal registers to both

4   the ALU and the encryption execution unit;

5   providing a multiplexer having inputs from both the ALU and the encryption exe-

6   cution unit, the multiplexer outputting a selected input.

1   29.   (Previously Presented) The method of Claim 27 further comprising the step of:

2   initializing the encryption TCSM unit in response to a first instruction that defines

3   a form of operation to be performed.

30. (Previously Presented) The method of Claim 29, wherein the step of initializing comprises the steps of:

decoding a first portion of the first instruction to initialize a DES functional component; and

decoding a second portion of the first instruction to initialize a sub-key generation functional component.

31. (Previously Presented) The method of Claim 27, further comprising the steps of:

executing a second instruction including an encryption opcode that specifies loading an initial key from a memory into a sub-key generation functional component of the TCSM unit.

32. (Currently Amended) The method of Claim 27, further comprising the steps of:

performing a DES function in response to execution of a third instruction having a field containing an encryption opcode that specifies loading plaintext and initializing [initalizing] a DES operation.

1   33.   (Currently Amended) A computer readable media, comprising:

2   said computer readable media containing instructions for execution in a processor

3   for the practice of the method of,

4   _____providing a tightly-coupling hardware data encryption function with software-

5   based protocol decode processing within a pipelined processor of a programmable proc-

6   essing engine in a network switch;

7   providing an encryption execution unit within the pipelined processor;

8   providing an ALU within the pipelined processor;

9   enabling, by an instruction decode stage (ID stage) [ALU] in response to read-

10   ing an opcode [op-code], the encryption execution unit to read data from a memory

11   shared by the ALU and the pipelined processor, and for the encryption execution unit to

12   process the data read from the memory; and

13   selecting as output the result of processing by the encryption execution unit rather

14   than selecting results from the ALU.

1   34.   (Currently Amended) Electromagnetic signals propagating on a computer net-

2   work, comprising:

3   said electromagnetic signals carrying instructions for execution on a processor for

4   the practice of the method of,

5   _____providing a tightly-coupling hardware data encryption function with software-

6   based protocol decode processing within a pipelined processor of a programmable proc-

7   essing engine in a network switch;

8   providing an encryption execution unit within the pipelined processor;

9   providing an ALU within the pipelined processor;

10   enabling, by an <u>instruction decode stage (ID stage)</u> [ALU] in response to reading

11   an <u>opcode</u> [op-code], the encryption execution unit to read data from a memory shared

12   by the ALU and the pipelined processor, and for the encryption execution unit to process

13   the data read from the memory; and

14   selecting as output the result of processing by the encryption execution unit rather

15   than selecting results from the ALU.

---

1   35. (Currently Amended) A router, comprising:

2   a processor having an <u>instruction decode stage (ID stage)</u> [ALU] for processing

3   <u>opcodes</u> [op-codes];

4   [and]

5   <u>an ALU for performing protocol processing operations;</u>

6   _____a tightly coupled state machine (TCSM) for performing encryption processing;

7   a shared memory for providing data to either the ALU or the TCSM;

8   the <u>ID stage</u> [ALU] , in response to reading an <u>opcode</u> [op-code], transferring

9   processing to the TCSM, and the TCSM performing encryption processing on data read

10   from the shared memory;

11   a selector to select as output results from the ALU OR results from the TCSM.

1   36. (Previously Presented) The apparatus of Claim 35, further comprising:

2   the selector is a multiplexer.

1   37. (Previously Presented) The apparatus of Claim 35, further comprising;

2   the ALU selects whether the ALU or the TCSM reads data from the memory.

1   38. (Previously Presented) The apparatus of Claim 35, further comprising:

2   the TCSM performs DES data encryption standard encryption processing.

1   39. (Previously Presented) The apparatus of Claim 35, further comprising:

2   a sub-key generation component to provide a key to the TCSM.

1   40. (Currently Amended) A method for operating a router, comprising:

2   [providing a processor having an ALU for]

3   processing [op-codes] opcodes by an instruction decode stage (ID stage); [and]

4   [a tightly coupled state machine (TCSM) for]

5   performing encryption processing by a tightly coupled state machine (TCSM);

6   performing protocol processing by an ALU;

7   reading data from a shared memory by either the ALU or the TCSM;

8   transferring processing by the ID stage [ALU], in response to reading an opcode

9   [op-code,] to the TCSM, and the TCSM performing encryption processing on data read

10   from the shared memory;

11   selecting as output results from the ALU OR results from the TCSM.

1   41. (Previously Presented) The method of Claim 40, further comprising:

16

2   using a multiplexer for selecting as output results from the ALU OR results from

3   the TCSM.

1   42. (Currently Amended) The method of Claim 40, further comprising;

2   selecting [by the ALU] whether the ALU or the TCSM reads data from the

3   memory.

1   43. (Previously Presented) The method of Claim 40, further comprising:

2   performing DES data encryption standard encryption processing by the TCSM.

1   44. (Currently Amended) The method of Claim 40, further comprising:

2   providing a key to the TCSM by a sub-key generation component.

1   45. (Currently Amended) A router, comprising:

2   means for providing a processor having an ALU for processing opcodes [op-

3   codes] and a tightly coupled state machine (TCSM) for performing encryption process-

4   ing;

5   means for reading data from a shared memory by either the ALU or the TCSM;

6   means for transferring processing by an instruction decode stage (ID stage) [the

7   ALU], in response to reading an opcode [op-code], to the TCSM, and the TCSM per-

8   forming encryption processing on data read from the shared memory;

9   means for selecting as output results from the ALU OR results from the TCSM.

17

1   46. (Previously Presented) The apparatus of Claim 45, further comprising:

2   means for using a multiplexer for selecting as output results from the ALU OR

3   results from the TCSM.

1   47. (Previously Presented) The apparatus of Claim 45, further comprising;

2   means for selecting by the ALU whether the ALU or the TCSM reads data from

3   the memory.

1   48. (Previously Presented) The apparatus of Claim 45, further comprising:

2   means for performing DES data encryption standard encryption processing by the

3   TCSM.

1   49. (Currently Amended) The apparatus of Claim 45, further comprising:

2   means for providing a key to the TCSM by a sub-key generation component.

1   50. (Currently Amended) A computer readable media, comprising:

2   said computer readable media containing instructions for execution in a processor

3   for the practice of the method of,

4   providing encryption functions within a pipelined processor in a network switch,

5   having the steps,

6   associating a first set of opcodes with an ALU internal to the processor, the ALU

7   performing protocol processing operations;

8   associating a second set of opcodes with an encryption execution unit internal to

9   the processor, the encryption execution unit performing encryption operations;

10

11   [having an encryption tightly coupled state machine (TCSM), wherein protocol process-

12   ing operations are performed by the ALU and encryption operations are performed by the

13   encryption execution unit in response to said second set of opcodes; and]

14   decoding opcodes by an instruction decode stage (ID stage);

15   transferring by the ID stage, in response to an opcode from the first set of op-

16   codes, processing to the ALU;

17

18   transferring by the ID stage [ALU], in response to an [op-code] opcode from

19   said second set of opcodes, processing to the encryption execution unit

20   [to process encryption operations in response to said second set of opcodes]; and

21   selecting output from the ALU OR from the encryption execution unit.

1   51. (Currently Amended) Electromagnetic signals propagating on a computer network,

2   comprising:

3   said electromagnetic signals carrying instructions for execution on a processor for

4   the practice of the method of,

5 providing encryption functions within a pipelined processor in a network switch,

6 having the steps,

7 associating a first set of opcodes with an ALU internal to the processor, the ALU

8 performing protocol processing operations;

9 associating a second set of opcodes with an encryption execution unit internal to

10 the processor, the encryption execution unit performing encryption operations;

11 [having an encryption tightly coupled state machine (TCSM), wherein protocol process-

12 ing operations are performed by the ALU and encryption operations are performed by the

13 encryption execution unit in response to said second set of opcodes; and]

14

15 decoding opcodes by an instruction decode stage (ID stage);

16 transferring by the ID stage, in response to an opcode from the first set of op-

17 codes, processing to the ALU;

18

19 transferring by the ID stage [ALU], in response to an [op-code] opcode from

20 said second set of opcodes, processing to the encryption execution unit

21 [to process encryption operations in response to said second set of opcodes]; and

22

23 selecting output from the ALU OR from the encryption execution unit.

1 52. (Currently Amended) A computer readable media, comprising:

2 said computer readable media containing instructions for execution in a processor

3 for the practice of the method of operating a router, having the steps,

4 [providing a processor having an ALU for]

20

5   processing opcodes <u>by an instruction decode stage (ID stage);</u> [and]

6   [a tightly coupled state machine (TCSM) for]

7   performing encryption processing <u>by a tightly coupled state machine (TCSM)</u>;

8   <u>performing protocol processing by an ALU;</u>

9   reading data from a shared memory by either the ALU or the TCSM;

10   transferring processing by the <u>ID stage</u> [ALU], in response to reading an <u>opcode</u>

11   [op-code,] to the TCSM, and the TCSM performing encryption processing on data read

12   from the shared memory; <u>and</u>

13   selecting as output results from the ALU OR results from the TCSM.

1   /53. (Previously Presented) Electromagnetic signals propagating on a computer network,

2   comprising:

3   said electromagnetic signals carrying instructions for execution on a processor for

4   the practice of the method of operating a router, having the steps,

5   [providing a processor having an ALU for]

6   processing opcodes [op-codes] <u>by an instruction decode stage (ID s.͏ ͏e);</u> [and]

7

8   [a tightly coupled state machine (TCSM) for]

9   performing encryption processing <u>by a tightly coupled state machine (TCSM)</u>;

10   <u>performing protocol processing by an ALU;</u>

11   reading data from a shared memory by either the ALU or the TCSM;

12   transferring processing by the <u>ID stage</u> [ALU], in response to reading an <u>opcode</u>

13   [op-code,] to the TCSM, and the TCSM performing encryption processing on data read

14   from the shared memory; <u>and</u>

15   selecting as output results from the ALU OR results from the TCSM.